EXPERIMENT NO - 01

Name: Kale Komal Janardan

Div: TE IT – A

Roll No.: ITA539 **Batch: A2**

DOP: **Sign:**

DOS: **Grade:**

Aim: Breaking the mono-alphabetic substitution cipher using frequency analysis method.

About the experiment:

In this experiment, we work with another well-known historical encryption scheme, namely the mono-alphabetic substitution cipher that has a very large key space. However, it is quite easily broken using “Frequency analysis” methods. Your task is to break this cipher. Specifically, given (only) the cipher text in some instance of a mono alphabetic substitution cipher, you need to find the plain text and the secret key.

Theory:

Consider we have the plain text "cryptography". By using the substitution table below, wecan encrypt our plain text as follows:
abcd efgh ijkl mnop qrst uvwx yz

JIBR KTCN OFQY GAUZ HSVW MXLD EP

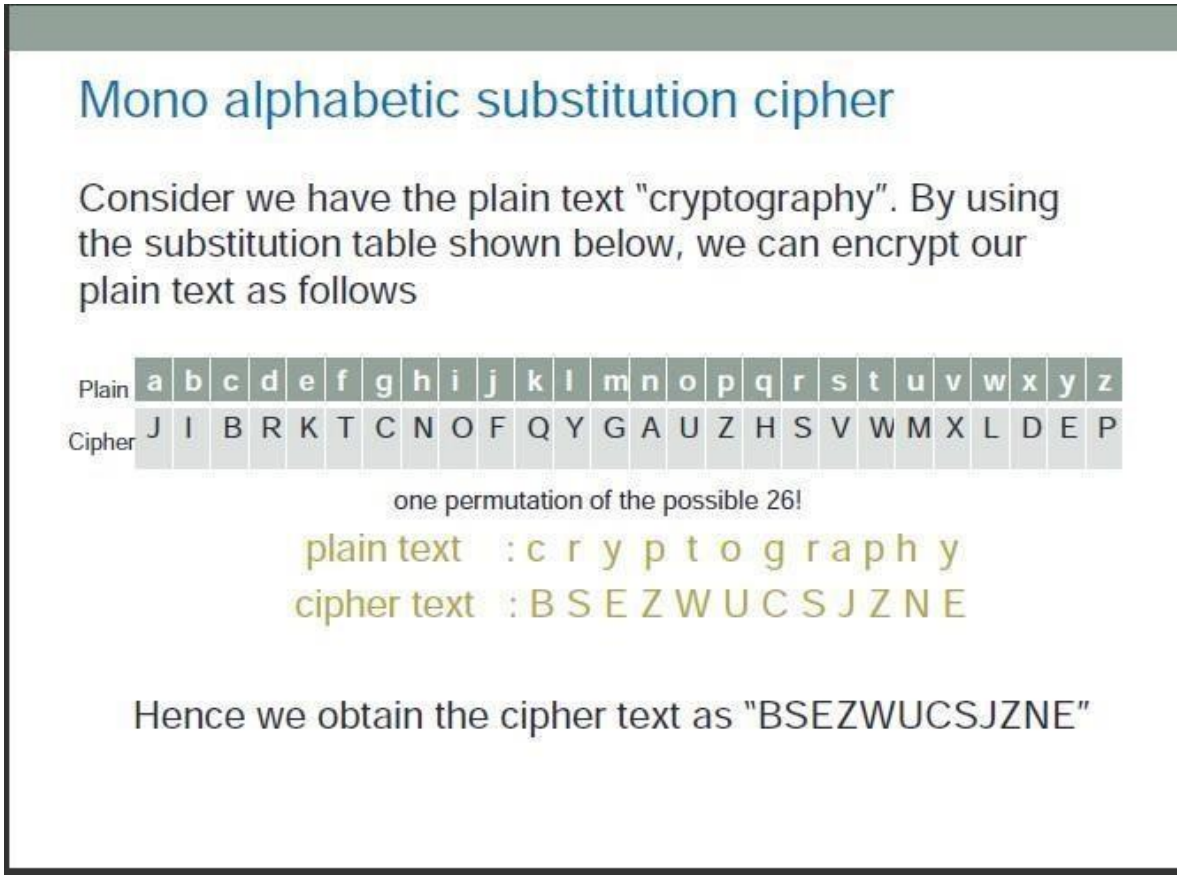
plain text: c r y p t o g r a p h y

cipher text: B S E Z W U C S J Z N E

Hence, we obtain the cipher text as “BSEZWUCSJZNE”.

Cryptanalysis

Note that the frequency of occurrence of characters in the plaintext is "preserved" in the cipher text. For instance, the most frequent character in the cipher text is likely to be the encryption of the plaintext character "e" which is the most frequently occurring character in English. For a very brief theory of the mono-alphabetic substitution cipher and its cryptanalysis.



Procedure:

STEP 1: For the given cipher text in the PART I of the experiment page, the first step is togenerate cipher text by clicking on the "Next Cipher Text" button.

STEP 2: Calculate frequencies of generated cipher text by clicking on "CalculateFrequencies in Cipher text" button.

STEP 3: Copy the generated cipher text from PART I and paste in "Scratchpad" area of PART II.

STEP 4: Analyze similarities between "Calculated Frequencies Table" and "EnglishAlphabet Frequencies Table".

STEP 5: Based on similarities, try to make a frequency-based estimation for each characterof cipher text.

STEP 6: Replace characters of Cipher Text in Scratchpad with a character estimatedpreviously using a Modify function of PART II.

STEP 7: Based on Hints from Cipher text in "Scratchpad" area make more replacement ofcipher text characters.

STEP 8: Repeat Step 7 till you get a meaningful English Text.

Simulation:

PART I:

PART I

Decrypt the following cipher text. A tool to simulate the Mono-Alphabetic Subsitution cipher is provided beneath for your assistance.

Here is the table of frequencies of English alphabets for your reference:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.167	1.49	2.782	4.253	12.702	2.228	2.015	6.094	6.966	0.153	0.772	4.025	2.406
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
6.749	7.507	1.929	0.095	5.987	6.327	9.056	2.758	0.978	2.360	0.150	1.974	0.074

```
dkxyvrh 1 - qegt vkr hxccwv keur: xuwdr wn cehrq nwvvwtp et vkr hwsrhcxto gwvk
krh nwnvrh, gkrt nkr tevwdrn x vxuowtp, duevkrq gkwvr hxccwv gwvk x yedorv
gxvdk hit yxnv. nkr leuuegn wv qegt x hxccwv keur gkrt niqqrtub nkr lxuun x
uetp gxb ve x dihwein kxuu gwvk fxtb uedorq qeehn el xuu nwmrn. nkr lwtqn x
nfxuu orb ve x qeeh vee nfxuu leh krh ve lwv, civ vkheipk gkwdk nkr nrrn xt
xvvhxdvwsr pxhqrt. nkr vkrt qwndesrhn x cevvur uxcruurq 'qhwto fr', vkr
detvrtvn el gkwdk dxinr krh ve nkhwto vee nfxuu ve hrxdk vkr orb. x dxor gwvk
'rxv fr' et wv dxinrn krh ve pheg ve nidk x vhrfrtqein nwmr krh krxq kwvn vkr
drwuwtp.
```

Next Ciphertext

Calculate Frequencies in ciphertext

Ciphertext Frequencies:

a	b	c	d	e	f	g	h	i	j	k	l	m
0.000	1.037	2.282	3.942	8.091	1.452	3.112	5.602	2.075	0.000	8.506	1.452	0.415
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
7.469	1.867	1.452	3.32	11.618	0.622	4.979	5.602	9.959	6.639	7.884	0.622	0.000

PART II:

PART II

Note that the *cipher text is in lower case* and when you replace any character, the final character of replacement, i.e., *plaintext is changed to upper case* automatically in the following scratchpad.

Scratchpad:

```
CHAPTER 1 - DOWN THE RABBIT HOLE: ALICE IS BORED SITTING ON THE
RIVERBANK WITH HER SISTER, WHEN SHE NOTICES A TALKING, CLOTHED WHITE
RABBIT WITH A POCKET WATCH RUN PAST. SHE FOLLOWS IT DOWN A RABBIT
HOLE WHEN SUDDENLY SHE FALLS A LONG WAY TO A CURIOUS HALL WITH
MANY LOCKED DOORS OF ALL SIZES. SHE FINDS A SMALL KEY TO A DOOR TOO
SMALL FOR HER TO FIT, BUT THROUGH WHICH SHE SEES AN ATTRACTIVE
GARDEN. SHE THEN DISCOVERS A BOTTLE LABELLED 'DRINK ME', THE CONTENTS
OF WHICH CAUSE HER TO SHRINK TOO SMALL TO REACH THE KEY. A CAKE WITH
'EAT ME' ON IT CAUSES HER TO GROW TO SUCH A TREMENDOUS SIZE HER HEAD
HITS THE CEILING.
```

Modify the text above (in scratchpad):

This is case *insensitive* function and replaces only cipher text (lower case) by plain text (upper case):

Replace cipher character [m] by plaintext character [z] Modify

Use the following function to undo any unwanted exchange by giving an uppercase character and a lower case. This is a case sensitive function:

Replace character [ ] by character [ ] Replace these exact characters

Your replacement history:

You replaced d by C You replaced k by H You replaced x by A You replaced y by P You replaced v by T You replaced r by E You replaced h by R You replaced c by B You replaced w by I You replaced e by O You replaced u by L You replaced q by D You replaced g by W You replaced t by N You replaced n by S You replaced s by V You replaced o by K You replaced p by G You replaced i by U You replaced l by F You replaced b by Y You replaced f by M You replaced m by Z

Conclusion:

Thus, we have studied how to break the Mono-alphabetic Substitution Cipher Successfully.